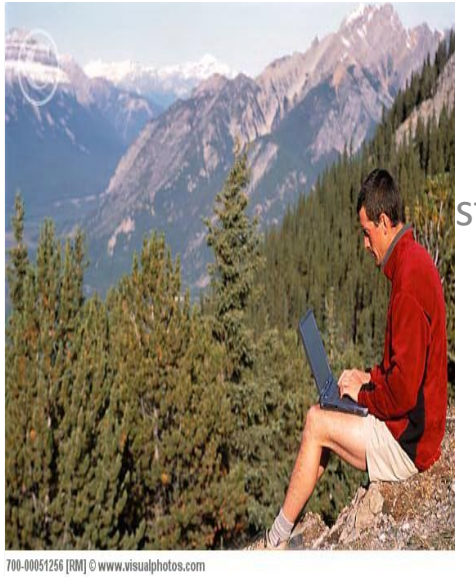
Enemy in the Wire(less):
T&E Perspectives on Wireless Security

Brief for the Naval Postgraduate School Wireless Technology Forum

Click

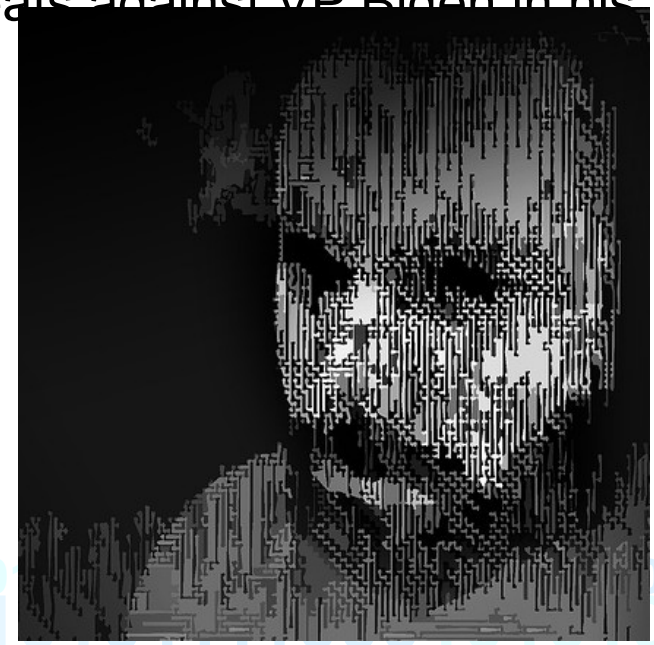


style

David J. Aland
19 July 2011

US v. Ardolf

- Barry Ardolf hacks his neighbor's WEP-protected wireless home network in retaliation for police complaint
  - "Certified Ethical Hacker", Internet technician for MedTronic
  - Downloads and uses "AirCrack" to reduce WiFi passwords
  - Creates fake accounts tied to victim identity, social network sites
  - Sends porn, nasty emails, and death threats against VP Biden in his victim's name with dire results for victim
  - NOT caught by Secret Service or police
  - Caught by a private security company
- **GUILTY** in Federal Court
  - 18 years in prison
  - no computer use until released
  - 20 years probabtion after release.



Hackers v. Wireless

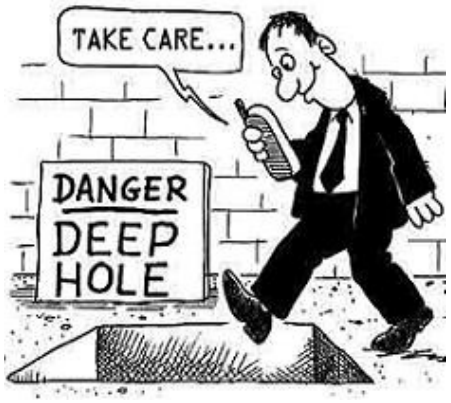
- Thomas Roth, University of Köln, Germany
  - Rents space on the Amazon Elastic Computer Cloud for $0.28/min
  - Generates 400,000 brute-force passwords per second
  - Breaks WEPs, averaging 6 min (approximate cost = $1.68 / network)
- CryptoCard, UK
  - Sends testers to coffeeshops to set up bogus WiFi hotspots
  - Captures an average of 350 usernames/passwords per hour
- Navy Research Lab, Washington DC
  - During BETA test of wireless discovery tool (with GPS/Google Maps), discovers internet thieves stealing wireless cash register data
- News of the World, UK
  - Hacks cell phones of celebs, politicians, 9/11 victims

Exercise IA Assessments

- DoD conducts IA assessments during major exercises with the support of the operational test agencies and the Information Warfare Centers
  - ATEC, 688TES, COMOPTEVFOR, MCOTEA, JITC
  - 1IOC, 24AF, 10TH FLT, MCNOSCC, NSA
  - `20-25 exercises per year at COCOMs and Services
- Results are aggregated and analyzed for enterprise level issues and recommendations
- “Smoking Gun” issues are sent as formal findings to cognizant Service or Agency at the 3-star level
- Annual trends are reported to DoD and Congress

Wireless and Mobile Tools

- Exercise assessments show three major issues with operational proliferation of common wireless/mobile tools:
  - Physical accountability and TEMPEST controls
    - Loss of physical control over a device loaded with sensitive data
    - Loss of CAC card and device credentials
    - Signal monitoring (quantity and quality)
  - Environmental Masking of effects and vulnerabilities
    - Only the most austere environments are wireless-free
    - Urban combat environments are wireless-dense
  - Stupid human tricks
    - Storing and transmitting PII or sensitive data
    - “Pretending” the device is secure
    - Cross-infection techniques



To Secure or Not To Secure

- The majority of wireless/mobile devices in use in operational environments are not secure or meant to be
- Secured wireless devices like SME-PED are rare
- Therefore … the principal security problem is NOT:
  - Type I or Type II encryption
  - Multi-Level Security
  - Suite B compliance and effectiveness
- The principal security problem is that unsecured wireless/mobile devices are cheap, ubiquitous, and highly functional , and often misused

Technology is not the whole answer…

- Better device security is a MUST
  - Wireless devices will not just “go away” because they are tough to secure.
- Functional standards are needed as badly as technical standards
  - The first device to market may be attractive, but the competitor catch-ups are usually better provisioned
  - The device maker must have an incentive to build in safeguards that can be re-purposed for specialized security environments
  - Device management cannot be “iSourced” out or untouchable
  - An operational doctrine of Perishability should be applied to their use: handle data only appropriate to that level of operations, and only handle perishable data on portable devices

Conclusion

- Wireless mobile devices are here to stay (at least until we invent something even better)
- Wireless mobile devices provide an undeniable tactical advantage to combat forces as well as enviable convenience to senior decision makers
- Wireless mobile devices provide an almost indefensible vulnerability to any user, regardless of technical profile
- Use of perishable frequencies, “thin client” devices (Tech) as well as transitory information practices (SOP) can make the security technology gap less dangerous
  - *If speed is why you have a mobile device, use it to your advantage!*